## Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

## Listing of the Claims:

1. (Currently amended) A method of processing data encrypted according to an encryption method specific to a first domain such that the data cannot be decrypted without using a first secret specific to said first domain, said data being received in a presentation device connected to a network belonging to a second domain, the method comprising:

(a) transmitting at least a portion of said encrypted data to a processing device connected to the network;

(b) receiving, in said presentation device, processed data from said processing device, at least one element of said processed data being used by said presentation device to decrypt said received data using a second secret specific to said second domain, said second secret being contained in the presentation device, said second secret specific to said second domain being different from said first secret specific to said first domain; wherein

the data received in the presentation device are encrypted using a first symmetric key, said first symmetric key being received with said data in a form encrypted using the first secret;

step (a) comprises transmitting to the processing device the first symmetric key encrypted using the first secret; and

step (b) comprises receiving from the processing device:

said first symmetric key encrypted using a second symmetric key; and the second symmetric key encrypted using the second secret specific to the second domain; the method further comprising:

(c) decrypting, using the second secret, the second encrypted symmetric key;

(d) decrypting, using the second symmetric key, the first encrypted symmetric key; <u>and</u>

(e) decrypting the data received by said presentation device using the first symmetric key~~; and~~

~~(f) transmitting a portion of data in the clear containing viewing control information indicative of a right of said presentation device to copy received data~~.

2. (Cancelled).

3. (Cancelled).

4. (Previously presented) The method as claimed in claim 1, comprising, before step (a), generating a random number,

said random number being transmitted to the processing device, in step (a), with the encryption of the first symmetric key;

wherein the data received in step (b) contain a random number and the first symmetric key encrypted using the second symmetric key;

step (d) also comprising the decryption, using the second symmetric key, of an encrypted random number received in step (b); and

further comprising, before step (e), verifying that the random number decrypted in step (d) is identical to the random number generated before step (a).

5. (Previously presented) The method as claimed in claim 1, wherein a domain identifier is contained in the data received by the presentation device and

further wherein said domain identifier is transmitted to the processing device during step (a).

6. (previously presented) The method as claimed in claim 1 further comprising initially applying a hash function to said portion of encrypted data and said portion of data transmitted in the clear prior to encryption of said portion of encrypted data.

7. (previously presented) The method as claimed in claim 1 wherein said second domain comprises a local domestic network of presentation devices.